REMARKS

In the Official Action mailed 01 May 2008, the Examiner reviewed claims 2-4, 6, 7, 9-11, 13, 14, 16-18, 20, 21 and 31-39. The Examiner has rejected claims 37-39 under 35 U.S.C. §112, first paragraph; and has rejected claims 2-4, 6, 7, 9-11, 13, 14, 16-18, 20, 21 and 31-39 under 35 U.S.C. §103(a).

No claims are amended. Claims 2-4, 6, 7, 9-11, 13, 14, 16-18, 20, 21 and 31-39 remain pending.

Applicant has also amended the specification to correct typographical errors noticed by Applicant upon review of the application.

Each rejection is respectfully traversed below.

Rejection of Claims 37-39 under 35 U.S.C. §112, first paragraph

The Examiner has rejected claims 37-39 under 35 U.S.C. §112, first paragraph as failing to comply with the written description requirement. Reconsideration is requested.

Specifically, the Office Action states that these claims fail to comply with the written description requirement, based on the assertion the "machine readable data storage medium" is not described in the application as filed. This is clearly mistaken. The original application as filed includes claims 15-21, which recited an article of manufacture comprising a machine readable data storage medium. It is well settled that the original specification for the purpose of the written description requirement in 35 U.S.C. §112, first paragraph, includes the original claims. So, the original application shows that the inventor was in "possession of the claimed invention" at the time of filing, and claims 36-39 comply with the requirement.

The rejection also suggests that the term in not clear. However, since the rejection is not presented under 35 U.S.C. §112, second paragraph, Applicant presumes that the comment is just rhetoric, and not a rejection for indefiniteness. Furthermore, Applicant submits that the term "machine readable data storage medium" is clear to persons of skill in the art. Any rejection of these claims on this basis would not be supportable. It is well understood in the art that computer programs of the type described in the present application are embodied in a machine readable data storage medium.

Accordingly, reconsideration of the rejection of claims 37-39 as amended is respectfully requested.

Rejection of Claims 2-4, 6, 7, 9-11, 13, 14, 16-18, 20, 21 and 31-39 under 35 U.S.C. §103(a)

The Examiner has rejected claims 2-4, 6, 7, 9-11, 13, 14, 16-18, 20, 21 and 31-39 under 35 U.S.C. §103(a) as being unpatentable over Perlman (US 6,363,480) in view of Kelly (US 5,636,280), and further in view of Official Notice. Reconsideration is requested.

Objection to Official Notice

Applicant objects to the Official Notice stated at page 7, at the 6th and 5th lines from the bottom, reading "The nth and (n+1)th iterations also includes creating a hash of the session key, which the Examiner takes the Official Notice to be also a well-known technique in the art." Specifically, it is not clear what the "noticed fact" is intended to be. The Official Notice purports to paraphrase the claimed "first set of exchanges", but does so inaccurately. The "first set of exchanges" does not include nth and (n+1)th exchanges. Also, the claim does not recite a hash of the session key. Examiner has confused the "first set of exchanges" with the "second set of exchanges, and has confused the intermediate data keys with the session key of the claim. This confusion contributes to the inability for Applicant to know exactly what the Examiner believes is the well-known prior art. Second, even assuming that the Examiner intended for the Official Notice to apply to the claimed "first set of exchanges", the "first set of exchanges" recites a specific use of a hashed version of an intermediate data key. It is unclear whether the Examiner is taking a position that the specific claim limitation is well-known prior art, a position simply that the use of hashed data is well-known in the abstract, or some intermediate position about the use of hashed data an iterative algorithm.

Accordingly, Applicant objects to the Official Notice, because the "noticed fact" is not clearly stated. Applicant submits that the Examiner should provide documentary evidence so the "noticed fact" can be deciphered, and placed in clear context.

Basis of Request for Reconsideration

Reconsideration is requested. The Office Action has not set forth the rationale for using the combination of steps recited in the claim. Rather, the Office Action is based on the approach

of addressing each of the steps taken alone. Therefore, the *prima facie* case relied upon by the Examiner can be characterized as a "picking and choosing" case. Specifically, the elements set forth in the Office Action are chosen, and in some cases misinterpreted, from the two references in the record that perform separate functions unrelated to the claimed invention and vague Official Notice, parts of the references are then are pieced together in a manner only possible in light of the present specification, and then a conclusion is presented without reasoning tied to the combination of steps recited in the claims, that the claims as a whole would have been obvious.

This "picking and choosing" case is rebutted herein by addressing the classic flaw in such reasoning. Specifically, the claims herein are non-obvious over this set of references because the claim elements in combination perform a function not found in the prior art, and "do not merely perform the function that each element [corresponding elements in the prior art chosen by the Examiner] performs separately." See, "Examination Guidelines for Determining Obviousness Under 35 USC 103 in View of the Supreme Court Decision in KSR International Co. v. Teleflex Inc.", Federal Register, Vol. 72, No. 195, pp. 57526-57535, issued by the United States Patent and Trademark Office on October 10, 2007 (the "USPTO Guidelines"), page 57534, at the end of the third column.

The present claims provide a combination of elements which perform a function unlike any in the prior art. Specifically, the claims provide a process for generating and distributing ephemeral keys, combined with mutual authentication, where the keys are generated at the first station without reliance on preset keys. The fact that there is no reliance on preset keys is seen in the claims, by the fact that the keys generated at the first station and sent to the second station are used for encryption in all the claimed instances of encryption in the claim. The fact that the final symmetric key is ephemeral is seen from the context of the claim. The mutual authentication is explicit in the claim as well. No reference in the record provides these combined functions. Indeed, no reference in the record describes a protocol similar the that in the claims for any purpose.

The picking and choosing case presented by the Office Action is addressed in detail below, with reference to the corresponding portions of claim 31, which starts as follows:

> **31. (previously presented) A method for mutual authentication in communications between first and second stations, comprising:**

generating and storing a set of ephemeral session keys at the first station, ephemeral session keys in the set being associated with respective session key initiation intervals, and being discarded at a time later than expiration of the respective session key initiation intervals;

The Office Action takes the position that this limitation reads on Perlman at "Fig. 1 and the associated text, particularly col. 5 lines 10-25". The Examiner is not properly interpreting the phrase "session key initiation intervals". In Perlman, the key pairs shown in Fig. 1 of the Perlman patent have respective “expiration times”. The passage at column 5, lines 10-25 describes the basic structure of the table in Fig. 1, and that the key pairs are "irretrievably destroyed at the associated expiration time." In claim 31, it is clear that the "session key initiation interval" is not an expiration time. The claim specifically states that the "ephemeral session keys" are "discarded at a time later than the expiration of the respective session key initiation intervals." The "session key initiation interval" in claim 31 is a time during which the particular session key will be used for initiation of a session. This error in interpretation is compounded in the rationalization of the rejection of claim 4, where the Office Action distinguishes between the initiation interval and the expiration time. A coherent rejection of these claims cannot have it both ways.

The idea of when a key can be used for initiation of the session and the idea of when a key expires are basically different. This difference between the initiation interval in the claim and an expiration time is more pronounced in the next limitation of the claim which reads:

in response to a request to initiate a communication session received by the first station during a particular session key initiation interval, selecting the associated session key;

In the process of claim 31, the "associated session key" is selected based on the session key initiation interval in which a request to initiate a communication session is received. In Perlman, a key is selected from the list by "the second party" which selects a key based on its expiration time or who provides an expiration time to the "first party" which in turn selects a key from the list based on the expiration time. See, column 6, lines 1-20. The expiration time of the

key selected in a system of Perlman is not relevant to the point in time at which the second party requests initiation of a session.

The Examiner takes the position that this limitation reads on the subject matter in Perlman at column 6, lines 1-20. It is clear therefore, that the Examiner is taking an interpretation of "session key initiation interval" in claim 31 as reading on the "expiration time" of Perlman. This interpretation is incorrect, because the "session key initiation interval" refers to an interval of time in which a request for establishing a session is received, rather than a time in which the encryption key will expire. In Perlman, the key is selected based on whether it will have a lifetime sufficient to meet the needs of the communication session, as indicated by its expiration time. According to claim 31, an "associated session key" is selected based on the time at which a request to initiate a session is received. The "associated session key" is selected independent of any user parameters. The key selected in Perlman is selected explicitly with the expiration time that the second party specifies. It can be seen therefore that the claimed "session key initiation interval" and the "expiration time" of the key in Perlman are fundamentally different.

The next limitation in claim 31 reads:

> **sending a message carrying said associated session key to the second station, and receiving a response from the second station including a digital identifier, the digital identifier being information shared between the first station and the second station, or between the first station and a user at the second station, the digital identifier being encrypted using said associated session key to verify receipt of the session key by the second station and to identify the second station or the user of the second station;**

The Office Action sites Perlman, column 6, lines 21-35, noting the discussion in Perlman column 2, lines 20-35 of the use of the SSL protocol which the Office Action characterizes as suggesting "using short-term keys (ephemeral) in setting up a session key." The Office Action acknowledges that Perlman does not discuss sending a message including a digital identifier encrypted using the associated session key. However, the Office Action suggests that it would be obvious to persons of skill with knowledge of Kelly.

In general, we would agree that it is known in the art, to exchange an encryption key using a short-term keys, such as apparently applied in the SSL protocol. However, this general knowledge does not suggest using an "associated session key" selected as required in claim 31 in this manner for encryption of a digital identifier for the purpose recited in the claim. Specifically, and unlike the prior art, the associated session key is used to encrypt the digital identifier, and sent back to the first station, not to hide the digital identifier, but rather to verify receipt by the second station of the session key. The rationale set forth by the Examiner ignores this stated feature in the claim. Therefore, Applicant submits that the reliance on Kelly and Perlman in this context is both misplaced and incomplete. Furthermore, the Office Action ignores the relationship of this claim limitation with the other limitations in the claim.

The next limitation in claim 31 reads:

> **generating and storing, in the first station, a set of intermediate data keys, the set of intermediate data keys including intermediate data key (i), for i = 1 to at least n, and being discarded at a time later than expiration of the particular session key initiation interval;**

With respect to this limitation, the Office Action states "this limitation creates n ephemeral keys, with the same characteristics of Perlman's ephemeral keys discussed above. An iterative process, which repeats the same steps, and how it is taught in the prior art is discussed in the following." Office Action, page 6.

From this just quoted comment, Applicant surmises that the Examiner is reading the claim limitation "set of intermediate data keys" on keys other than the selected key in the table of Fig. 1 in Perlman. This interpretation is flawed because it ignores the manner in which the intermediate data keys are utilized as part of a single communication session as required by subsequent limitations of the claim, and because there is no suggestion in Perlman that more than one of the keys in the table of Fig. 1 would be used together for any purpose. Rather, the keys in Perlman are selected for independent sessions. The flaw of this interpretation is more apparent from analysis of additional limitations in the claim below.

At the next limitation in claim 31 reads:

> **executing a first set of exchanges including one or more exchanges with the second station, after verifying in said first station receipt of the session key by the second station by decrypting the digital identifier using the associated session key at the first station and positively matching the decrypted digital identifier against an existing entry in a stored list of authorized users,**

The Office Action cites Kelly for the proposition that a digital identifier exchanged in this manner will be verified against the database. Again, in general this is a well-known function in communication systems. However, the Office Action does not establish the process of using an associated session key selected as required by the claim for this purpose. This remains a fundamental problem with the Examiner's interpretation of the claim as discussed above.

The claim goes on to define further details of the first set of exchanges as follows:

> **the first set of exchanges including**
>
> **sending a message to the second station carrying intermediate data key (i) from said set of intermediate data keys encrypted using the associated session key for a first exchange in first set of exchanges and using the intermediate data key (i-1) for subsequent exchanges in the first set of exchanges,**
>
> **receiving a response from the second station including a hashed version of intermediate data key (i) encrypted using intermediate data key (i), decrypting the hashed version of the intermediate data key (i), calculating a hashed version of intermediate data key (i) at the first station, and matching the calculated hashed version and the received hashed version of intermediate data key (i) to verify receipt by the second station of intermediate data key (i);**

With respect to this sequence of steps recited in claim 31, the Office Action paraphrases this limitation, stating "In other words, the above process is an iterative method, which involves application of a set of operations in each iteration, each of those operations identical to one of the operations discussed above. Namely, and during the first to the (n-1)th iteration, the system repeat sending a new key, encrypted from one station to the other. The new key is encrypted

with a key known to both parties (the previous session key). The receiving side decrypts the encrypted new key and uses it as the session key Column 5, lines 55-column 6, lines 20. Perlman's teaching of ephemeral keys is for the purpose of substituting a key with another after the lifetime of a key is expired. Therefore, the session keys are substituted with a fresh key after expiration of their lifetime. This whole process is discussed above."

Claim 31 does not state that one key is replaced by another after its lifetime is expired. Indeed, the limitations in claim 31 to which the Examiner's comments are addressed describe an exchange of messages which is completely different than anything in Perlman. There is no process described in Perlman that involves sending one of the keys from the table in Fig. 1 encrypted using another of those keys. Furthermore, Perlman requires that the second party actively select keys from the table based on their desired expiration time. This act of selecting a key is completely independent of any other key that that user may have selected in the past. It is not true that "session keys are substituted with a fresh key after expiration of their lifetime" as stated by the Examiner, in any process described in Perlman. The idea that Perlman shows an iterative process like that of the "first set of exchanges" in claim 31 is simply incorrect.

The Examiner's comments on the claim limitations related to the "first set of exchanges" in claim 31 goes on to state "This whole process is discussed in the above." Applicant does not understand this comment, and requests clarification should the Examiner maintain this rejection on reconsideration.

The Examiner's comments on the "first set of exchanges" in claim 31 continues with the statement: "In the nth and (n+1)th iteration, the same process continues, with the exception that in the nth iteration the shared secret is used to encrypt the new key, and in the (n+1)th iteration a second shared secret is used for the same. This technique is also discussed above." In this comment, that Examiner is confusing the "first set of exchanges" with the "second set of exchanges" in claim 31. In the first set of exchanges, the shared secret is not recited in the claim.

Also, Applicant does not understand the Examiner's comment "This technique is also discussed above." Neither the technique being referred to, nor the discussion being referred to is clear to Applicant.

Applicant points out that the claim includes a first set of exchanges in which the intermediate data keys are utilized, and a second set of exchanges in which the shared secrets are

utilized. The Office Action provides no rationale for a finding that a protocol using these two sets of exchanges would be obvious.

Continuing with reference to the limitation related to the "first set of exchanges", the Office Action includes the following statement: "The nth and (n+1)th iterations also includes creating a hash of the session key, which the Examiner takes the Official Notice to be also a well-known technique in the art."

Applicant objects to the Official Notice as discussed above. It is clear that the use of hashed data is in general a known technique widely used in the computer industry for many purposes. However, there is no evidence that the prior art has applied the technique in the manner recited here.

As stated above, it is not clear what the "noticed fact" is intended to be. First, the "first set of exchanges" does not include nth and (n+1)th exchanges. Also, the claim does not include a hash of the session key. Examiner has confused the "first set of exchanges" with the "second set of exchanges, and has confused the intermediate data keys with the session key of the claim. This confusion contributes to the inability for Applicant to know exactly what the Examiner believes is the well-known prior art.

Examiner concludes with reference to the "first set of exchanges" as follows: "Therefore, all steps of the iterative method are discussed, and shown as prior art in the above. Also, using an iterative technique to improve the security of the cryptographic protocol is well-known in the art. Reference is made to the DES protocol, which basically deploys a plurality of stages that scrambles the input data iteratively, and each iterative stage uses a different parameter (HT) to perform a different operation. The key in each stage is extracted from the previous stage. As another example, reference is made to "Applied Cryptography" by B. Schneier, page 53 (a copy is attached to this Office Action). Section titled SKEY, clearly teaches the concept of repeated application of the cryptographic technique to improve the security of the protocol. Therefore, given enough resources and time, it would have been obvious to use and here it method, which includes a well-known process at each iterative stage to improve the security of the protocol."

This passage by the Examiner is an apparent reliance on the fact that iteration is a well-known technique in the abstract. The citation to the DES protocol and the citation to the SKEY process of Schneier merely establish that perhaps iteration is used in cryptography. However, these references have nothing to do with the specific protocol recited in claim 31, which requires

first selecting a session key based on the session key initiation interval in which a request is received, followed by a set of exchanges using a sequence of intermediate keys using the recited combination of hashing, iteration, and the key generation.

Claim 31 goes on to recite a second set of exchanges as follows:

executing a second set of exchanges for mutual authentication after verifying in said first station receipt of the intermediate data key (n-1) by the second station, including

sending a first message carrying intermediate data key (n) encrypted using a hashed version of a first shared secret,

receiving a response from the second station carrying a hashed version of intermediate data key (n) encrypted using a hashed version of the first shared secret, and decrypting the hashed version of the intermediate data key (n) , calculating a hashed version of intermediate data key (n) at the first station, and matching the calculated hashed version and the decrypted hashed version of intermediate data key (n) to verify possession by the second station of the first shared secret;

sending a second message carrying intermediate data key (n) encrypted using a hashed version of a second shared secret; and

if the second station sends a response to the second message, carrying a hashed version of intermediate data key (n) encrypted using a hashed version of the second shared secret, after possession by the first station of the second shared secret is verified at the second station, the verifying being accomplished at the second station by decrypting the intermediate data key (n) from the second message using the hashed version of the second shared secret, calculating a hashed version of the intermediate data key (n), and matching the calculated hashed version and the decrypted hashed version of intermediate data key (n) to verify possession by the first station of the second shared secret, then

receiving the response from the second station, and decrypting the hashed version of the intermediate data key (n) using the hashed version of the

second shared secret, calculating a hashed version of intermediate data key (n) at the first station, and matching the calculated hashed version and the decrypted hashed version of intermediate data key (n) at the first station to verify mutual authentication of the first and second stations; and

With respect to this sequence of steps, the Office Action merely states "(the second set of exchanges again involves an iteration process, similar to what is discussed above, with a difference of using a second shared secret in addition to the first shared secret, and using a hashed version of an encryption key to encrypt the key. However, using the second shared secret is again repeating the same process where the first secret is used. Also use out a hashed version of a plea is known in the art, as exemplified in DES protocol.)" Office Action, page 9.

Applicant points out that the Examiner is again mischaracterizing the claim limitation. The "first set exchanges" does not use a shared secret as this passage by the Examiner appears to suggest. The "second set of exchanges" is the only place in which the first and second shared secrets are utilized in the claim. To characterize that the second set of exchanges is essentially the same as the first, where the Examiner has misunderstood the first set exchanges is clear error.

Furthermore, this statement seems to characterize the "second set of exchanges" as essentially the same as the "first set of exchanges". However, review of the claim shows that they are substantially different, that they include different combinations of steps, and that they provide completely different functions for the claimed protocol. In fact, the statement that the iteration using the second shared secret "is again repeating the same process where the first secret is used", is not correct. The exchange of messages involving the first shared secret is used by the first station to authenticate the second station. The exchange of messages involving the second shared secret is used to support authentication of the first station by the second. Thus, the steps are different, and the claim recites the difference. Accordingly, the *prima facie* case based on this mischaracterization of the claim is flawed and should be withdrawn.

The final claim limitation reads as follows:

if mutual authentication is verified at the first station, then sending a message indicating successful authentication.

As to this limitation, the Examiner refers to Kelly at column 6, lines 57-52. This is a concluding step for the authentication protocol and will occur in any robust authentication system. Kelley does not however both perform authentication, and provide an ephemeral symmetric encryption key as is accomplished using the process of claim 31.

Claim 31 provides a detailed protocol for providing both mutual authentication and an ephemeral symmetric encryption key that is highly secure and scalable for use in large-scale secure data networks. Neither Perlman nor Kelly provides this combination of functions.

Furthermore, the Office Action has not set forth the rationale for using the combination of steps recited. Rather, it is based on the approach of addressing each of the steps taken alone. Specifically, the elements set forth in the Office Action are chosen from the two references in the record that perform separate functions unrelated to the claimed invention, and vague Official Notice, and the chosen elements are pieced together in a manner only possible in light of the present claims, and then a conclusion is presented without clear reasoning that the claims would have been obvious.

The Office Action suffers the classic flaw in such reasoning. Specifically, the claims herein are non-obvious over this set of references because the claim elements in combination perform a function not found in the prior art, and "do not merely perform the function that each element [corresponding elements in the prior art chosen by the Examiner] performs separately." See, USPTO Guidelines, page 57534, at the end of the third column.

Perlman provides ephemeral keys, but they are not selected as required by the claim based on a session key initiation interval. Perlman provides many keys, but does not associate them together in an iterative protocol as claimed herein for delivering a symmetric encryption key. Kelly describes an authentication protocol, and thus has some features related to authentication like the present claims. But the process of Kelly does not relate to distribution of symmetric keys, and does not provide authentication without preset keys like the claimed process. The Office Notice about hashing, to the extent we can guess about its scope, is again not related to the claimed process.

Likewise, neither Perlman nor Kelly discuss a protocol for distributing symmetric encryption keys, much less one like that recited in claim 31 involving mutual authentication.

Claim 31 in particular, and all the present claims provide a combination of elements which perform mutual authentication and key distribution, unlike any in the prior art.

Claims 32, 33, 2-4, 6, and 7 depend from claim 31 and are patentable for at least the same reasons. In addition, each recites a unique and unobvious combination as discussed below.

Turning to claim 32, the Office Action rejects this claim with the rationale "encryption using a key such as key (n-1) was well known in the art at the time of the invention. The motivation to do so would be to secure the message by delivering it in ciphertext rather than clear text." This rationale for rejection suggest that the mere fact that it is desirable to encrypt a message proves that it is obvious to do so in the specific manner claimed. The rejection is flawed because it does not address the specific limitation in the claim that requires the use of a specific intermediate data key, that had been used earlier for another specific purpose. These limitations in the claim have been ignored in the rejection, and therefore the *prima facie* case is incomplete and flawed.

Turning to claim 33, the Office Action states "the purpose of establishing keys between parties of communication is encrypting the message for the purpose of confidentiality protection, or integrity protection". This comment is not a rationalization for finding of obviousness. In fact, Perlman and Kelly do not relate to the distribution of symmetrical encryption key. Neither reference even describes a technique for doing so. The Official Notice appears to be related to the use of a hash algorithm in general. Therefore, to the extent that it can be understood, it is also unrelated to symmetric encryption keys. Therefore, the *prima facie* case for rejection of claim 32 is incomplete and flawed.

Turning to claim 2, Applicant points out that this claim recites a characteristic of the session key initiation interval and the associated session key which is unlike anything in the prior art. The Examiner overlooks the fact that the session key is associated with the particular session key initiation interval, and selected based on that association. There is no similar process described in Perlman as discussed in detail above with respect to claim 31. Furthermore, the idea expressed in claim 2 of using the same session key for different communication sessions with different parties, because the request for initiation of the sessions occurred during the same interval of time is completely different than anything in the prior art. This also suggests the unique and an inventive character of the process using the associated session key recited in these claims.

Turning the claim 3, it depends from claim 2, and is patentable for the reasons mentioned above. In addition, the rejection is flawed because the Examiner reads the intermediate data keys on the set of keys presented in the algorithm of Perlman. The Examiner has not provided any explanation of how Perlman suggests using the any keys in a process like that recited in the present claims. Furthermore, the keys described in Perlman are final encryption keys, not applied to any iterative process, as mentioned above in connection with the rejection of claim 31. Therefore, the rejection is incomplete and should be withdrawn.

Turning to claim 4, the rejection includes the following statement: "setting the lifetime such that it is usable after the set up period is completed is a obvious, logical and trivial choice. It is a trivial choice to choose the lifetime of session keys to be longer than the initiation interval because the initiation interval is part of the session." This comment demonstrates a fundamental error made by the Examiner. Specifically, in the analysis of the session key initiation interval in claim 31, the Examiner read the "session key initiation interval" on the expiration time of the keys in Perlman. With respect to claim 4, the Examiner is taking a position that the initiation interval is different than the lifetime. Any coherent rejection of these claims cannot have it both ways. In fact, the concept of an initiation interval that is associated with a session key used as claimed herein, is not found in Perlman or any of the references in the record. Reconsideration and withdrawal of the rejection of these claims is therefore requested.

Claim 6 depends from claim 4 and provides further definition of the session key lifetimes, establishing them from the initiation intervals. Thus, claim 6 is patentable for at least the reasons discussed above in connection with claim 4.

Claim 7 provides characterization of parameter for limiting the lifetime of a session key. It is patentable for at least the same reasons as claim 4, from which it depends, as discussed above. Also, the Office Action relies on the generic idea that the lifetime of a key must be long enough to accomplish its function. This generic idea provides no teaching whatsoever of a limit on the lifetime of the key as recited in claim 7.

The parallel claims sets are rejected in the Office Action by reference to the analysis of claims 31, 32, 33, 2-4, 6, and 7. Applicant submits that such claims are patentable as discussed above.

Accordingly, reconsideration of the rejection of claims 2-4, 6, 7, 9-11, 13, 14, 16-18, 20, 21 and 31-39 as amended is respectfully requested.

CONCLUSION

It is respectfully submitted that this application is now in condition for allowance, and such action is requested.

The Commissioner is hereby authorized to charge any fee determined to be due in connection with this communication, or credit any overpayment, to our Deposit Account No. 50-0869 (AIDT 1005-1).

Respectfully submitted,

Dated: 28 July 2008

/Mark A. Haynes/

Mark A. Haynes, Reg. No. 30,846

HAYNES BEFFEL & WOLFELD LLP
P.O. Box 366
Half Moon Bay, CA 94019
(650) 712-0340 phone
(650) 712-0263 fax